COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Media Protection (MP) controls

CMS requirements for Administering Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Purpose **2**
Background **3**
Affordable Care Act 3
CMS oversight 3
ARC-AMPE 3
Control mapping **4**
Media Protection (MP) 4
References **9**
Legal disclaimer **10**

Purpose

This white paper provides a guide for Administering Entities (AEs) to upgrade their System Security and Privacy Plans (SSPPs) from the Minimum Acceptable Risk Standards for Exchanges (MARS-E) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Media Protection controls:

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	51
Awareness and Training	9
Audit and Accountability	19
Assessment, Authorization, and Monitoring	12
Configuration Management	31
Contingency Planning	23
Identification and Authentication	24
Incident Response	16
Maintenance	16
Media Protection (This Document)	**9**
Physical and Environmental Protection	19
Planning	6
Program Management	28
Personnel Security	9
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	12
System and Services Acquisition	34
System and Communications Protection	34
System and Information Integrity	34
Supply Chain Risk Management	6

Background

Affordable Care Act

The Affordable Care Act (ACA) revolutionized access to healthcare in the United States by establishing Health Insurance Marketplaces (HIMs). Enhanced Direct Enrollment (EDE) is an ACA innovation that allows third-party entities, such as insurers and web-brokers, to offer consumers a seamless application and enrollment experience directly through their platforms. This approach improves accessibility to the marketplace while maintaining compliance with federal regulations.

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of AEs, which are responsible for overseeing and managing marketplace operations to ensure compliance with federal regulations, safeguard consumer data, and maintain the integrity of the HIM. Key aspects of CMS's oversight include:

- Requiring AEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the AE environment to ensure the confidentiality, integrity, and availability of consumer data and requiring entities to implement cybersecurity controls, conduct regular risk assessments, and submit independent security audits.
- Requiring AEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring AEs to report any data breaches or system incidents promptly and to take corrective actions as directed by CMS and the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).
- Requiring AEs to renew their Authority to Connect (ATC) or Authority to Operate (ATO) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that AEs in the healthcare.gov environment deliver secure, compliant, and user-friendly services, aligning with the ACA's mission to expand access to quality health coverage.

ARC-AMPE

CMS published the ARC-AMPE Version 1.02 on April 9, 2025. This framework is slated to replace the Minimum Acceptable Risk Standards for Exchange (MARS-E) security and privacy guidelines:

- ARC-AMPE Volume 1 contains high-level guidance, and Volume 2 has the minimum-level security and privacy controls.
- ARC-AMPE Volume 2 is the new format for the SSPP for ACA AEs.
- AEs must have ARC-AMPE implemented by March 4, 2026.
- The implementation date for EDE entities has yet to be announced as of the date of this white paper.

The minimum control baseline for ARC-AMPE compliance consists of 402 controls which have been derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

The number of controls required represents a significant increase from the MARS-E baseline, and AEs should be prepared for an increased level of effort for developing the SSPP and to submit more artifacts during audits.

Another major change is the format of the SSPP template. MARS-E uses a Microsoft Word format whereas ARC-AMPE is an Excel spreadsheet.

Control mapping

The mapping of the controls found in MARS-E Version 2.2 (based on NIST SP 800-53 Revision 4) to their new locations in ARC-AMPE (based on NIST SP 800-53 Revision 5) are included in the table below. The table lists the MARS-E control directly compared with the ARC-AMPE equivalent control name, as applicable. The table also documents any new ARC-AMPE controls that do not have MARS-E equivalents, as well as those controls that have been combined or withdrawn for ARC-AMPE.

Note also that all references to NIST SP 800-53 Revision 5 included below are based on version 5.1.1, which was issued on November 7, 2023.

Media Protection (MP)

The set of controls in this family focus on how the Exchange shall: (1) protect IT system media, both paper and digital; (2) limit access to information on IT system media to authorized users; and (3) sanitize or destroy IT system media before disposal or release for reuse.

MARS-E		ARC-AMPE	
Control	**Media Protection Policy and Procedures**	**Control**	**Policy and Procedures**
MP-1: Media Protection Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel, including employees and contractors with potential access to Personally Identifiable Information (PII): **1.** A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the media protection policy and associated media protection controls. **b.** Reviews and updates (as necessary) the current: **1.** Media protection policy within every three hundred sixty-five (365) days; and **2.** Media protection procedures within every three hundred sixty-five (365) days. **Implementation Standards** **1.** Semi-annual inventories of removable media containing PII are conducted. The organization accounts for any missing removal media containing PII by documenting the search efforts and notifying the media initiator of the loss. **2.** Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital		**MP-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level media protection policy that: **(a)** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **(b)** Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and **2.** Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; **b.** Designate organization-defined officials to manage the development, documentation, and dissemination of the media protection policy and procedures; and **c.** Review and update the current media protection: **1.** Policy at least every one (1) year and following organization-defined events; and **2.** Procedures at least every one (1) year and following organization-defined events.	

MARS-E		ARC-AMPE	
video disks) and non-digital media (e.g., paper and microfilm).			
Control	**Media Access**	**Control**	**Media Access**
MP-2: Media Access The organization restricts access to sensitive digital and non-digital media (which includes media containing PII) to defined personnel or roles (defined in the applicable security plan) by disabling: **a.** CD/DVD writers and allowing access to using CD/DVD viewing and downloading capabilities only to persons specified or in defined roles; and **b.** USB ports and allowing access to using USB device capabilities only to persons specified or in defined roles. **Implementation Standards** **1.** Define types of digital and non-digital media. **2.** Define a list of individuals with authorized access to defined media types. **3.** Define the types of security measures to be used in protecting defined media types. **4.** Defined personnel or roles must be authorized individuals with a valid need to know.		**MP-02: Media Access** Restrict access to all types of digital and non-digital media to organization-defined personnel or roles.	
Control	**Media Marking**	**Control**	**Media Marking**
MP-3: Media Marking The organization: **a.** Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and **b.** Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking if the media remain within a secure environment. **Implementation Standards** Do not exempt any removable media types from marking.		**MP-03: Media Marking** **a.** Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and **b.** Exempt specific types of media or hardware components, as specified, in writing, by the Chief Information Officer (CIO) or their designated representative, from marking if the media remains within a secure environment.	
Control	**Media Storage**	**Control**	**Media Storage**
MP-4: Media Storage The organization: **a.** Physically controls and securely stores all magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks within organization-defined controlled areas; encrypts digital media via a FIPS 140-2 compliant encryption module; and for non-digital media, provides secure storage in locked cabinets or safes. **b.** Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **c.** Digital and non-digital media includes removable media that contains PII This media must be stored in a securable area or in a locked container.		**MP-04: Media Storage** **a.** Physically control and securely store digital and/or non-digital media: all magnetic tapes, external removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks. Securely store digital and non-digital media within organization-defined controlled areas; and **b.** Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	

MARS-E		ARC-AMPE	
Implementation Standard **1.** If PII and PHI is recorded on magnetic media with other data, it should be protected as if it were entirely PII or PHI. **2.** Defines controlled areas within facilities where the information and information system reside.			
Control	**Media Transport**	**Control**	**Media Transport**
MP-5: Media Transport The organization: **a.** Protects and controls digital and non-digital media containing sensitive information, such as PII, during transport outside of controlled areas using cryptography and tamper-evident packaging, and **1.** If hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or **2.** If shipped, trackable with receipt by commercial carrier. **b.** Maintains accountability for information system media during transport outside of controlled areas; **c.** Documents activities associated with the transport of information system media; and **d.** Restricts the activities associated with the transport of information system media to authorized personnel. **e.** The organization protects and controls digital media that contains PII during transport outside of controlled areas using FIPS-validated encryption. **Implementation Standard** **1.** Protect and control non-digital PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Non-digital PII must be in locked cabinets or sealed packing cartons while in transit. **2.** The organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas, and encrypts digital media via a FIPS 140-2 compliant encryption module. **3.** The organization defines security measures to protect digital and non-digital media in transport.		**MP-05: Media Transport** **a.** Protect and control digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using organization-defined controls such as: • Most current FIPS 140-compliant encryption module; • Locked/securable containers or tamper-evident packaging transported via authorized personnel; • A trackable receipt by the commercial shipping carrier; and • Sealed packing cartons for non-digital media containing sensitive information. **b.** Maintain accountability for system media during transport outside of controlled areas; **c.** Document activities associated with the transport of system media; and **d.** Restrict the activities associated with the transport of system media to authorized personnel.	
Control	**Cryptographic Protection**	**Control**	**N/A**
MP-5 (4): Cryptographic Protection The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		Withdrawn control: Incorporated into **SC-28(01)**	
Control	**Media Sanitization**	**Control**	**Media Sanitization**
MP-6: Media Sanitization The organization: **a.** Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization		**MP-06: Media Sanitization** **a.** Sanitize digital and non-digital system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
c. The organization sanitizes digital media that contains PII prior to disposal, release out of organizational control, or release for reuse using FIPS-validated media sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.

Implementation Standard
1. Employ sanitization mechanisms consistent with guidance provided in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.
2. Finely shred hard-copy documents using approved equipment, techniques, and procedures, and employs cross-cut shredding at a minimum.
3. Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
a. Date received;
b. Reel/cartridge control number contents;
c. Number of records, if available;
d. Movement; and
e. If disposed of, the date and method of disposition.
4. Surplus equipment is stored securely while not in use and disposed of or sanitized in accordance with NIST SP 800 88 guidance, Guidelines for Media Sanitization, as amended when no longer required.
5. For Cloud Environment, the hypervisor enforces sanitization of the instance (container) image file space upon release:
a. Sanitization of released space is compliant with NIST SP 800-88 guidance, Guidelines for Media Sanitization, as amended.</td><td colspan="2">procedures in accordance with the most current NIST SP 800-88 guidelines; and
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.</td></tr>
<tr><td>Control</td><td>Review/Approve/Track/Document/Verify</td><td>Control</td><td>Review, Approve, Track, Document, and Verify</td></tr>
<tr><td colspan="2">MP-6(1): Review/Approve/Track/Document/Verify
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Implementation Standard
The organization ensures PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.</td><td colspan="2">MP-06(01): Review, Approve, Track, Document, and Verify
Review, approve, track, document, and verify media sanitization and disposal actions.</td></tr>
<tr><td>Control</td><td>Equipment Testing</td><td>Control</td><td>Equipment Testing</td></tr>
<tr><td colspan="2">MP-6 (2): Equipment Testing – Enhancement</td><td colspan="2">MP-06(02): Equipment Testing</td></tr>
</table>

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the equipment is achieving the intended sanitization.</td><td colspan="2">Test sanitization equipment and procedures within every one (1) year to ensure that the organization achieves the intended sanitization.</td></tr>
<tr><td>Control</td><td>Media Use</td><td>Control</td><td>Media Use</td></tr>
<tr><td colspan="2">MP-7: Media Use
The organization:
a. Prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).
b. Restricts the use of portable storage and mobile devices on information systems and networks containing PII, without using device ownership, media sanitization and encryption controls.</td><td colspan="2">MP-07: Media Use
a. Prohibit the use of personally owned media (e.g., flash drives, external hard disk drives, and other portable storage and media devices) on organization-defined systems and networks using organization-defined security safeguards; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.</td></tr>
<tr><td>Control</td><td>Prohibit Use Without Owner</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">MP-7 (1): Prohibit Use Without Owner
The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.</td><td colspan="2">Withdrawn control: Incorporated into MP-07.</td></tr>
<tr><td>Control</td><td>Media Related Records</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">MP-CMS-1: Media Related Records
Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information. The media-related records shall contain sufficient information to reconstruct the data in the event of a breach.

Implementation Standard
1. The media records must, at a minimum, contain:
a. The name of media recipient;
b. Signature of media recipient;
c. Date/time media received;
d. Media control number and contents;
e. Movement or routing information; and
f. If disposed of, the date, time, and method of destruction.</td><td colspan="2">There is no corresponding control in NIST 800-53/ARC-AMPE. Policies and procedures for media related records should be addressed in MP-01.</td></tr>
</table>

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the authors

Jessica Payne, Consultant

Jessica joined Coalfire in 2024 with five prior years of cybersecurity consulting experience. She supports our clients as a Consultant for the GRC Healthcare team where she specializes in cybersecurity risk management, cybersecurity program advisory, and compliance for the healthcare industry.

Her extensive experience in cybersecurity consulting allows her to provide customized solutions and guidance on industry best practices, greatly improving client security postures and ensuring compliance with regulatory standards. She is dedicated to ongoing improvement and to staying abreast of the latest cybersecurity trends and technologies to offer innovative solutions to her clients.

Ian Walters, Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST SP 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_ACA CMS Controls Migration (Media Protection (MP))_03102025